DAS

Iowa Department of Administrative Services

Government's Partner in Achieving Results

Chester J. Culver, Governor
Patty Judge, Lt. Governor

Ray Walton, Director

State of Iowa Enterprise Laptop Data Protection Security Standard

June 11, 2009

Purpose

This standard establishes the minimum security requirements for laptop computers and the data stored on, processed by, or transmitted via laptops.

Overview

Laptop computers provide users with the benefits of portability, flexibility, and increased productivity. Laptop computers allow users to take computers and data with them wherever they go. Laptop computers are an important tool for personnel that work at remote customer locations or are required to travel.

The benefits of laptop computers, however, come with potential risks. Due to their portability, a significant source of risk is the loss or theft of devices and the exposure of information stored on those devices. Also due to their mobile nature, these devices may connect to potentially hostile environments that lack adequate protections, subjecting the devices to attacks or potential infections, which may in turn be brought back to a State of Iowa network.

Scope

This standard sets minimum security and encryption requirements for laptop and tablet computers that hold state-owned data or connect to state-owned or managed networks. Laptops of contractors, state business partners and individuals connecting to state networks or storing state data are covered by this standard.

For the purpose of this standard, security is defined as the ability to protect the integrity, confidentiality and availability of information processed, stored and transmitted by an agency.

This standard applies to all agencies as defined by Iowa Code Chapter 8A, Section 101. Non-participating agencies are encouraged to follow this and other enterprise level policies, standards, guidelines, processes and procedures.

Definitions

Selected terms used in the Enterprise Laptop Data Protection Standard are defined below:

Laptop Computer: Laptop computers are lightweight, portable devices designed to operate for extended periods of time with a self-contained power source. For the purpose of this standard, a laptop computer includes devices classified as tablet computers.

- **Encryption:** The process of making information indecipherable to protect it from unauthorized viewing or use, especially during transmission or storage. Encryption is based on an algorithm and at least one key. Even if the algorithm is known, the information cannot be decrypted without the key(s).

Updates

This document will be reviewed at least every two years and updated as needed.

Enterprise Laptop Standard

Improperly configured laptop computers can expose sensitive or confidential data to unauthorized access and are vulnerable to malicious software. To ensure that data is protected, the following minimum standards must be met for all laptop computers:

1. **Laptop Inventory.** Agencies will maintain an inventory of all laptop computers and their assigned user.

2. **Data Encryption and Authentication.** All laptop computers must be encrypted. The encryption software must meet the following criteria:

    a. Pre-boot: Pre-boot user authentication must be used by the encryption software.
    b. Whole-disk: The entire hard drive shall be encrypted.
    c. Encryption Strength: 256-bit Advanced Encryption Standard (AES) or stronger encryption must be used.
    d. Audit Trail: An audit trail shall be maintained to demonstrate that a device was encrypted and the type of encryption software used.
    e. Central Management: The encryption process and procedures shall be centrally managed at the agency and/or enterprise level.
    f. Hibernation: Laptop encrypts upon hibernation requiring the user to re-authenticate.

3. **Loss/Theft Procedures.** Loss or theft of any laptop computer shall be reported to the Chief Information Security Officer within 24 hours. The notification shall include:
    a. Agency name and contact.
    b. Date of theft/loss.
    c. Description of the theft/loss.
    d. Whether confidential/sensitive information was stored on the device.
    e. Whether the laptop was encrypted.

    Procedures should also be in place to change authentication credentials to any systems the device may have accessed; including non-state-owned as well as state-owned devices which store sensitive or confidential data.

4. **Physical Protection.** Users of laptop computers are responsible for their physical protection.
    a. Use of cable locks and other physical security devices are encouraged where appropriate.
    b. Laptops shall not be left unattended in unlocked vehicles.

5. **Passwords**: Strong passwords must be used with laptops. Written passwords, smart cards, or tokens shall not be stored with the laptop.

6. **Primary Storage/Data Backups.** To ensure data availability in the event of device loss or theft, a laptop computer should not be the only or primary storage device for State of Iowa data. Frequent and regular backups of data stored on laptops must be made, according to agency policy.

7. **Client security maintained.** All laptop computers must have:
    a. A properly-configured host-based firewall;
    b. Up-to-date antivirus software; and
    c. The latest software patches.

8. **Assessment.** The ISO will periodically conduct assessments of agency compliance with this standard. Agencies will provide access to inventory information and systems as required to determine compliance. If violations of the laptop computer standard are identified, the agency will receive written notification pursuant to IAC 11--25.11(8A).

9. **Awareness Training:** Laptop computer users shall be provided with mobile security awareness training. At a minimum, users shall be provided with documentation describing mobile computing risks.

Effective Date This standard shall be effective September 1, 2009.

Enforcement This standard shall be enforced pursuant to Iowa Administrative Code 11—25.11(8A).

Variance Iowa Administrative Code 11 - 25.11(2) provides for variances from security standards. Requests for a variance from any of the requirements of this policy will be submitted in writing to the Chief Information Security Officer prior to implementation.